UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X
GENERAL BOARD OF GLOBAL MINISTRIES
OF THE UNITED METHODIST CHURCH

Petitioner,

MEMORANDUM OPINION
AND ORDER

-against-

CV 06-3669 (DRH) (ETB)

CABLEVISION LIGHTPATH, INC., et al.

Respondents.
----------X

Before the court is a motion to preclude respondent Cablevision from disclosing any records in its possession which relate to Ms. Lavonne Brown, and a Letter in Response to Petitioner's Memorandum in Support of Application for Disclosure Pursuant to FRCP Rule 27, filed by Ms. Lavonne Brown. Ms. Brown argues that it is a violation of her constitutional rights, including her right to privacy, for her internet service provider, Cablevision, to disclose any information pertaining to her internet service account. She also argues that petitioner "has no case." (Letter in Resp., dated Oct. 30, 2006.)

BACKGROUND

Petitioner filed a Petition to Perpetuate Testimony on July 26, 2006. The petition alleges that an unknown individual accessed the e-mail accounts of seven of petitioner's employees. (Petition ¶ 9, 12.) One of the employees whose e-mail account was accessed was Jan Love, the chief executive of petitioner's Women's Division. (Petition ¶ 9.) The petition alleges that the unknown individual accessed Ms. Love's e-mail account and sent

- in Ms. Love's name - an e-mail to three other employees, implying that the employees were going to be terminated. (Petition ¶ 9.) On June 8, 2006, an e-mail was sent that said "Ha, Ha, Ha – Guess who's positions will be eliminated on Monday, June 12th. Sorry for this. But you all should have done better work and had better attitudes! Good luck elsewhere!" (See Petition Exh. A.)

Once petitioner learned that Ms. Love's e-mail account had been accessed, petitioner's network administrator attempted to determine the identity of the person who sent the unauthorized e-mail message. (Petition ¶ 10.) The network administrator discovered that an unknown individual had, without authorization, accessed the e-mail accounts of seven employees between June 4 and June 8, 2006. (Petition ¶ 10.) The network administrator located the internet protocol ("IP") address of the unknown individual and reviewed records to determine whether accounts had been previously accessed through that IP address. (Petition ¶ 10, 12.) The network administrator determined that from April 21 through April 27, 2006, the individual with that IP address had accessed seven employee accounts on eleven occasions. (Petition ¶ 12.) The network administrator used an internet website to find the internet service provider ("ISP") for the IP address in question. Optimum Online of Cablevision Systems was identified as the internet service provider. (Petition ¶ 13.)

Petitioner contacted Cablevision and requested that Cablevision disclose the identity of the user with the IP address in question. Cablevision replied that it would not do so unless required to by court order. (Petition ¶ 14.) In addition, Cablevision told petitioner that it had a practice of deleting electronic records which would permit

Cablevision to identify the person with the IP address in question, within 90 days of the e-mail transaction. (Petition ¶ 15.)

On August 7, 2006, the undersigned entered an order directing Cablevision to preserve the information sought in the petition, pending further order of the court. (See Order of Judge E. Thomas Boyle, dated August 7, 2006.)

On September 5, 2006, the undersigned entered an order granting the petition to perpetuate testimony. On September 15, 2006 - but before any disclosure pursuant to the September 5, 2006 order - Ms. Lavonne Brown, acting pro se, came before the court with an Order to Show Cause, moving for an order enjoining petitioner from all attempts to perpetuate testimony from Cablevision and preventing Cablevision from disclosing records relating to her. (Mem. In Supp. Of Order to Show Cause.) Ms. Brown had received notification from Cablevision stating that it was going to disclose documents relating to Ms. Brown, in accordance with a court order. In a letter dated September 8, 2006, Cablevision said the information would be disclosed if the company did not receive a court order from Ms. Brown or her attorney. (See Letter from Cablevision to Ms. Brown, dated September 8, 2006.) On September 15, 2006, Judge Hurley entered an order preventing Cablevision from producing any records that relate to Ms. Brown until the undersigned had an opportunity to further address the matter. (Order of Judge Hurley, dated September 15, 2006.)

A conference was held before the undersigned on October 18, 2006. Ms. Brown did not appear, although notified. On October 25, 2006, petitioner filed a Memorandum in Support of Application for Disclosure Pursuant to FRCP Rule 27, arguing that petitioner is entitled to relief pursuant to 18 U.S.C. 2701, the Stored Communications

Act, and 18 U.S.C. 2707, which provides for a civil cause of action for violation of the Act. (See Mem. In Supp. of App. for Discl. at 2.) Petitioner argues that the petition has been plead in accordance with Fed. R. Civ. P. Rule 27. (Mem. In Support of App. for Discl. at 4.)

In a Letter in Response to Petitioner's Memorandum in Support of Application for Disclosure Pursuant to FRCP Rule 27, filed on November 2, 2006, Ms. Brown argues that the disclosure of her personal information by Cablevision will violate her right to privacy and her constitutional rights. (Letter in Response, dated October 30, 2006.) In its Reply, petitioner argues that Ms. Brown has not stated a constitutional basis for denying the requested relief. Also, petitioner argues that although Ms. Brown argues that she has not committed any wrongdoing, the purpose of the petition is simply to obtain discovery in order to identify the unknown individual as a party defendant in this action. (See Petitioner's Reply Mem. At 3-4.)

DISCUSSION

I. Stored Communications Act

The first issue is whether petitioner is bringing this claim under the proper statute. Petitioner claims relief pursuant to the Stored Communications Act ("SCA), 18 U.S.C. Section 2701. See Kaufman v. Nest Seekers, LLC, 2006 WL 2807177, at *3 (S.D.N.Y. Sept. 26, 2006). 18 U.S.C. Section 2707 provides for a civil cause of action for violation of Section 2701.

Section 2701(a) provides, in relevant part:

(a) Offense – . . . [W]hoever –

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

Section 2707(a) provides, in relevant part:

(a) Cause of action. . . . [A]ny provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

An "electronic communications service" is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. 2510(15). In re DoubleClick, Inc. Privacy Litigation, 154 F.Supp.2d 497, 508 (S.D.N.Y.2001). An electronic mail company is an electronic communications service. See State Wide Photocopy, Corp. V. Tokai Financial Service, Inc., 909 F.Supp.137, 145 (S.D.N.Y.1995). Communications in "electronic storage" are those temporarily stored by

electronic communications services incident to their transmission - "for example, when an e-mail service stores a message until the addressee downloads it." In re DoubleClick, 154 F.Supp.2d at 512.

The purpose of the SCA was, in part, to protect privacy interests in personal and proprietary information and to address "the growing problem of unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public." Kaufman v. Nest Seekers, LLC, 2006 WL 2807177, at *4 (S.D.N.Y. Sept. 26, 2006). SCA was designed to create a cause of action against computer hackers. See Kaufman, 2006 WL 2807177 at * 4; State Wide Photocopy, 909 F.Supp. at 145. Computer hackers are defined as electronic trespassers. See State Wide Photocopy, 909 F.Supp. at 145.

Petitioner has a computerized facility that provides an electronic communications service. Petitioner provided its employees with e-mail accounts for work purposes. (Petition ¶ 6, 7.) Petitioner alleges that communications in electronic storage were accessed. Petitioner maintains that an unknown defendant entered into the e-mail accounts of seven employees and gained access to "stored electronic communications" within those accounts. (Petition ¶ 9.) Petitioner alleges that the unknown defendant used such access to send e-mails in Ms. Love's name, purporting to terminate employees. (Memo. in Supp. Of app. For Discl. at 4.)

Petitioner asserts that the unknown individual was an electronic trespasser i.e., that such person entered into petitioner's e-mail accounts without authorization. (See Petition ¶ 10.)

For the foregoing reasons, petitioner's claim is properly brought under the Stored Communication Act.

II. Rule 27

The court must consider whether petitioner is entitled to perpetuate testimony under Fed. R. Civ. P. 27. Petitioner must show: (1) that it expects to be a party to an action that may be cognizable in a court of the United States but the action is unable to be brought presently; (2) the subject matter of the expected action and the petitioner's interest in such an action; (3) facts which the petitioner seeks to establish through the proposed testimony and the reasons for desiring to perpetuate that testimony at this time; (4) the names or description of the expected adverse parties and (5) the names and addresses of the witnesses to be examined and the substance of the testimony petitioner expects to obtain from those witnesses. Fed.R.Civ.P. 27(a)(1).

It is within the court's discretion to grant discovery pursuant to Rule 27. In Re Campania Chilena De Navegacion, 2004 WL 1084243, at *2 (E.D.N.Y. Feb. 6, 2006). A court may grant a Rule 27 petition "if it is satisfied that a failure or delay of justice may thereby be prevented." Messeller v. United States, 158 F.2d 380, 382 (2d Cir.1946).

Here, petitioner has demonstrated all the factors for Rule 27 except the fourth and fifth. At this time however, petitioner is unable to ascertain the names of adverse parties. This is the reason for the petition. Also, petitioner is not able to name witnesses. A petition may be granted in the absence of such information. See In Re Alpha Industries, Inc. 159 F.R.D. 456 (S.D.N.Y.1995) (granting rule 27 petition and discovery to allow petitioner to determine defendant in an action).

The identity of the unknown party defendant may be obtained through Cablevision, which is able to match the IP address to its subscriber. Furthermore, without court intervention, the information would be lost, since Cablevision routinely destroys such data in the ordinary course of its business after 90 days. See In Re: Town of Amenia, 200 FRD 200 (S.D.N.Y.2001) (granting Rule 27 petition and noting "[t]here is a significant risk that Mr. Selfridge's testimony will be lost if not perpetuated at this time.... [Such] expected testimony is highly valuable and no substitute source of the information which he may provide has been identified.").

III. Ms. Brown's Constitutional Rights

The court must consider whether granting the petition will violate Ms. Brown's constitutional rights. The unknown defendant is alleged to have used Cablevision's services to access the stored electronic communications of petitioner, without authorization. In addition, the unknown defendant logged into the e-mail account of an employee of petitioner and used that person's e-mail to send fictitious messages of termination to other employees. Such a person has a "minimal expectation of privacy," if any, in using an internet service provider to engage in such tortious conduct. See Sony Music Entertainment, Inc. V. Does 1-40, 326 F.Supp.2d 556 (S.D.N.Y.2004) ("defendants have little expectation of privacy in downloading and distributing copyrighted songs without permission").

Courts evaluating requests to identify information from ISPs regarding subscribers have considered a variety of factors to weigh the need for disclosure against First Amendment interests. See Sony Entertainment, 326 F.Supp.2d at 564-65. These

factors include: (1) a concrete showing of a prima facie claim of actionable harm (2) specificity of the discovery request (3) the absence of alternative means to obtain the subpoenaed information (4) a central need for the subpoenaed information to advance the claim, and (5) the party's expectation of privacy. Id.

A prima facie claim under SCA is established, discussed supra. The discovery request was made with specificity – petitioner is asking to perpetuate testimony to gain the identity of the holder of an IP address. (See Petition ¶ 16.) There are no other available means to obtain the information. Cablevision is the ISP and the only known entity with knowledge of the IP address that accessed petitioner's e-mail. (Petition ¶ 13.) Adequate need has been demonstrated. Lastly, as noted earlier, there is a minimal expectation of privacy in the alleged tortious conduct set forth in the petition. Thus, disclosure of information pertaining to the IP address does not violate the First Amendment.

CONCLUSION

For the foregoing reasons, I deny Ms. Brown's motion for a protective order and grant petitioner's application to perpetuate testimony, pursuant to Rule 27. Cablevision is directed to disclose information pertaining to the IP address requested in the Petition within 10 days.

SO ORDERED:

Dated: Central Islip, New York
November 30, 2006

/s/ E. Thomas Boyle
E. THOMAS BOYLE
United States Magistrate Judge